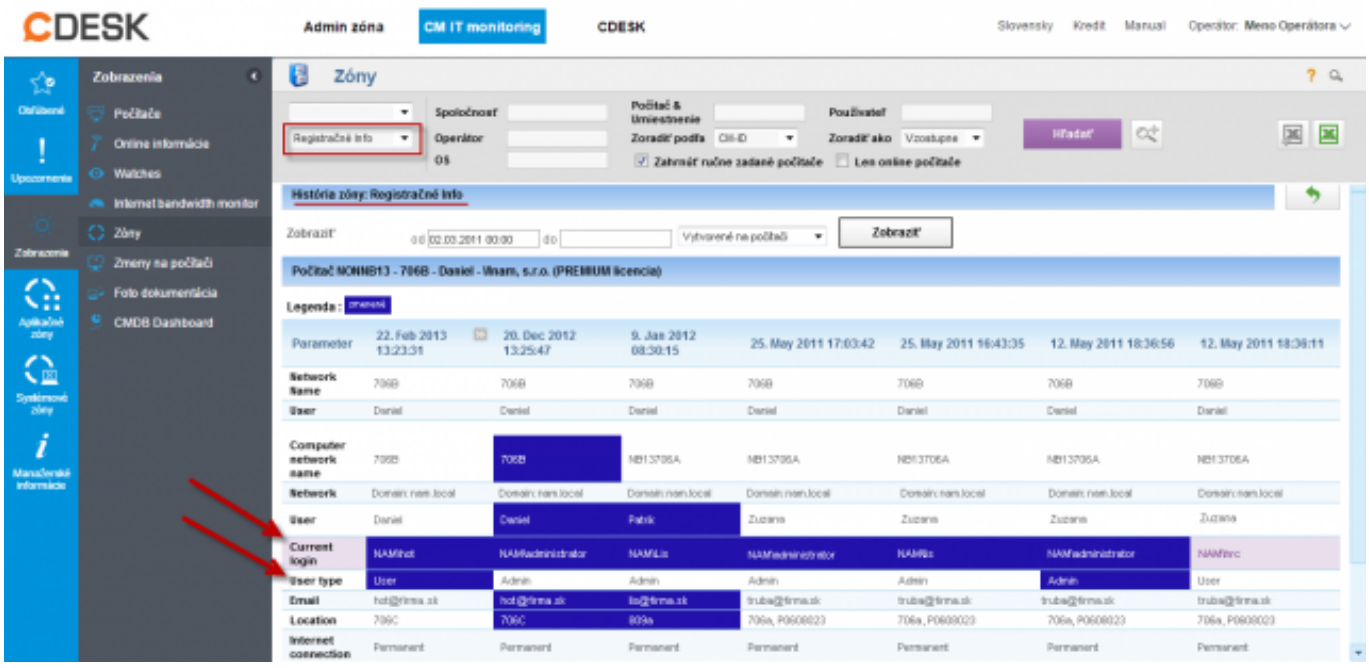
Prostredníctvom CM môžete lepšie zaistiť vašu počítačovú sieť, prípadne zistiť informácie súvisiace s bezpečnosťou nekolidujúce s ochranou informácií. Ponúkame vám zopár tipov na využitie tohto veľmi komplexného nástroja.

Výpis s historickými údajmi za posledných 6 mesiacov, aký typ používateľa sa prihlasuje

Otvorte si v CM CM IT monitoring -> Zóny -> Registračné info. K danému počítaču si otvorte histórі a uvidíte tam, kto sa kedy prihlásil s akými oprávneniami. Okrem toho tu vidíte aj zapamätané, kto mal daný počítač v používaní podľa CM registrácie, aké bolo sieťové meno počítača v minulosti. Zaujímavé informácie, ak potrebujete sledovať pohyb počítača po firme (tieto údaje budú zoskupené v CMDB)

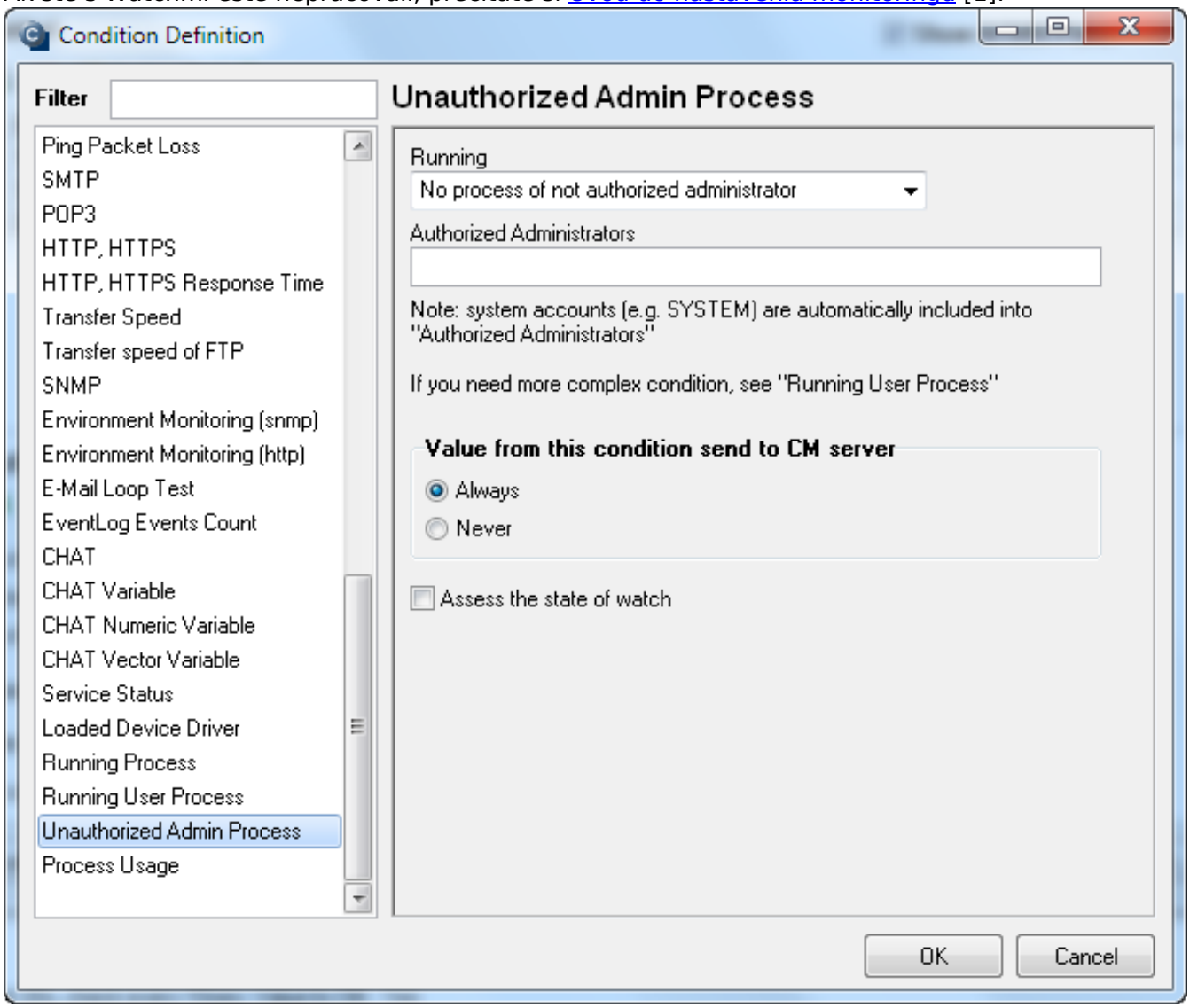


Obrázek: História počítača v Zóne Registračné info ukazaujúca okrem iného, aký používateľ bol s akými oprávneniami prihlásený.

Detekcia spusteného procesu s identitou neoprávneného administrátora

Vyššie popísaný prípad nezachytí, ak niekto na počítači spustí proces spôsobom Run As. Na tento prípad má CM prichystanú Watches podmienku Unauthorized Admin Process. Táto podmienka sleduje každých 30sekúnd, či nie je spustený akýkoľvek proces pod používateľom s administrátorskými oprávneniami mimo dovolených administraátorov. Efektívne aj voči prelomeniu účtu lokálneho administrátora. S touto podmienkou ustrážite spočítače, aby vám na ne šikovní

používatelia nepriinštalovali nebezbečné softvéry.
Ak ste s Watchmi ešte nepracovali, prečítate si Úvod do nastavenia monitoringu [1].

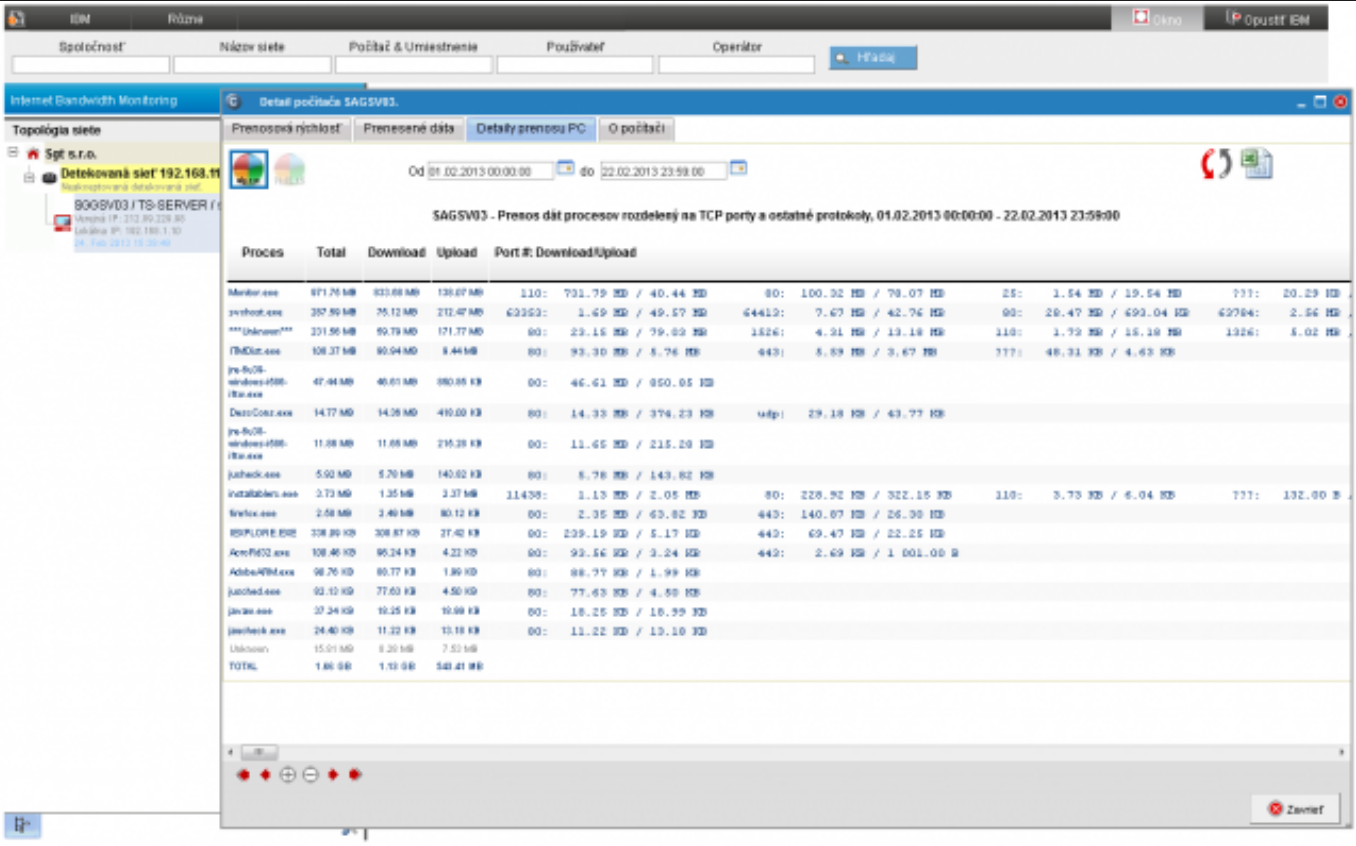


Obrázek: Watches podmienka (Condition) pre sledovanie spusteného procesu pod neautorizovaným administrátorom.

Monitorované sieťové prenosy s určením čísla portov a cieľovej IP adresy

Zaujímavé výstupy viete získať cez internet bandwith monitor. Ak máte podozrenie, že niekam systematicky unikajú údaje nedovoleným spôsobom, môžete to nájsť cez Internet Bandwith Monitor [2]. Nájdete tu prehľady internetových prenosov z jednotlivých aplikácií, na cieľové IP adresy, rozdelenie na porty. Prehľad prostredníctvom ktorého určíte, či nejaký pracovník nerobí systematicky nekalú činnosť.
Ak by vás zaujímalo, že či niekto nepreniesol príliš veľa údajov, sú na to aj Watches podmienky (Internet IP Trafic [3], Internet IP Transfered Data [4]).

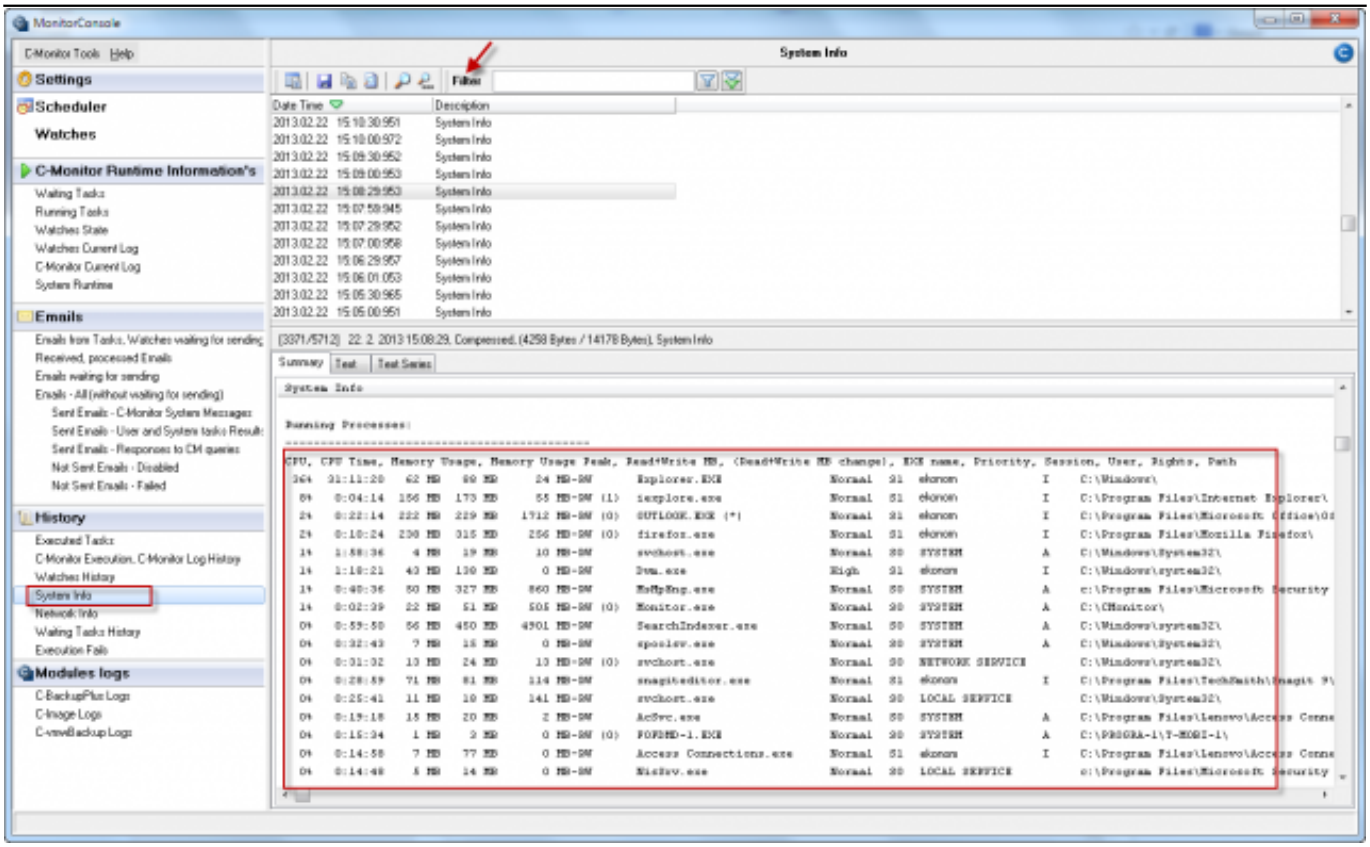
(v čase písania tohto príspevku sa spúšťa testovacia prevádzka už aj na všetkých 64bit systémoch okrem WIN8/ 2012. Doteraz boli podporené len 32bit systémy, takže záber tohto monitoringu je už dosť široký.)



Obrázek: Príklad výpisu prenesených dát cez internet jednotlivými aplikáciami

Zoznam procesov s určením vlastníka, ktoré sú spustené na počítači

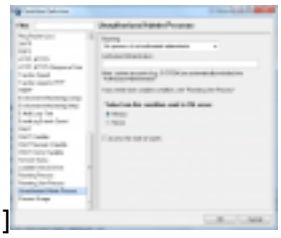
Bez akéhokoľvek nastavovania sa na počítači tvorí automaticky krátkodobá história (niekoľko dní dozadu každých 30sekúnd) dostupná cez C-MonitorConsole v Systémových informáciách. Ak potrebujete overiť, či bol spustený nejaký proces a s akými oprávneniami, tu ho nájdete. Procesy sa dajú aj dobre filtrovať, takže viete vidieť v akom intervale bol bol daný proces spustený. (História sa dá rozšíriť zväčšením archívu, ale má svoje limity, nakoľko toto nie je nástroj určený na detailné a dlhodobé sledovanie aktivity práce pracovníkov).
Viac informácií nájdete v článku Systémové info v rámci popisu C-MonitorConsole [5]



Obrázek: Prehľad spustených procesov cez uloženú krátkodobú históriu v System Info v C-MonitorConsole

Spúšťanie programom s admin.oprávneniami u používateľov "user" (funkčné aj na terminálových serveroch)

Mnohí administrátori tvrdia, že je nutné používateľom priradiť administrátorské oprávnenia, ak na počítači je program, ktorý korektne nefunguje bez admin. oprávnení alebo používatelia chcú robiť operácie, ktoré admin. oprávnenia vyžadujú. S C-Monitor-om už toto neplatí, lebo dokáže korektne spustiť program v profile používateľa "user" s oprávneniami administrátora. Je to stav, ktorému by sa ľudovo povedalo : Vlk bude sýty a ovca celá.
Spustenie programu vyžadujúceho admin.práva u používateľa, ktorý má odopreté admin.práva je ilustrovaný na BLOG článku **OpenVPN pre ne-admin používateľa** [6]
Date:
3.3.2012External Links:
Spustenie programu vyžadujúceho admin.práva u používateľa, ktorý má odopreté admin.práva [6]Obrázky:


[7]

[8]

[9]

[10]

Odkazy
[1] https://www.customermonitor.cz/ako-funguje-cm/monitoring-a-diagnostika/uvod-do-nastavenia-online-monitoringu-watches

[2] https://www.customermonitor.cz/ako-funguje-cm/monitoring/prenesene-data-cez-internet
[3] https://www.customermonitor.cz/ako-funguje-cm/monitoring-a-diagnostika/volby-a-nastavenie-watchov/prehlad-podmienok-conditions-watc#Internetiptraffic
[4] https://www.customermonitor.cz/ako-funguje-cm/monitoring-a-diagnostika/volby-a-nastavenie-watchov/prehlad-podmienok-conditions-watc#InternetIPTransferredData
[5] https://www.customermonitor.cz/ako-funguje-cm/cm-vnutorna-architektura/c-monitor-windows-klient/system-network-info
[6] https://www.customermonitor.cz/news/blog/openvpn-pre-ne-admin-pouzivatela
[7] https://www.customermonitor.cz/sites/default/files/OS_zona_registracne_info_Historia.png
[8] https://www.customermonitor.cz/sites/default/files/Watches_condition_Unauthorized%20Admin%20Process.png
[9] https://www.customermonitor.cz/sites/default/files/Internet_bandwith_Monitor_prehlad_prenosov_po_aplikaciach.png
[10] https://www.customermonitor.cz/sites/default/files/System_info_spustene_procesy.png